Cassandra Crossing/ Tor, brividi a lieto fine

(179)— L'attacco sferrato nei confronti di Tor non era probabilmente mirato a comprometterne il valore. Ma il network a cipolla ne èuscito…

Cassandra Crossing/ Tor, brividi a lieto fine

(179)— L'attacco sferrato nei confronti di Tor non era probabilmente mirato a comprometterne il valore. Ma il network a cipolla ne èuscito indenne: quando l'apertura e la trasparenza pagano.

29 gennaio 2010—E' tanto che Cassandra non la butta sul "tecnico", ed è una rarità che tragga da fatti di cronaca "nera" degli auspici positivi: oggi però una notizia importante ma trascurata dalla stampa e dai blog tecnici permetterà ambedue le cose.

La notizia è del 20 gennaio, quando i core developer del Progetto Tor hanno annunciato di aver scoperto che due dei server del Progetto Tor erano stati violati da cracker rimasti sconosciuti.

I due computer agivano sia da directory server (2 su un totale di 7) sia da repository dei sorgenti. I lettori che avessero bisogno di spiegazioni sul funzionamento di Tor possono far riferimento al sito del Progetto Tor ed alle mie "Lezioni di guida"

Non voglio sostituirmi alla lettura della mail in cui Roger Dingledine descrive dettagliatamente cosa è stato accertato e la portata precisa, per quanto è conoscibile, dell'evento. Per maggiori particolari ne consiglio la lettura, estesa magari all'intero thread su or-talk.

Voglio comunque riassumere e sottolineare alcuni punti chiave dell'intera vicenda.

1. [appare accertato che la violazione sia stata compiuta da cracker "casuali" che cercavano server potenti da usare per i loro scopi, ma che in realtà non intendevano in particolare attaccare Tor in quanto applicazione "critica".]
2. [è verificato che i sorgenti di Tor non sono stati alterati.]
3. [l'eventuale corruzione delle informazioni fornite in gennaio dai due directory server compromessi non avrebbe comunque causato nessun danno, perché le informazioni trasmesse dai dirserver vengono validate a maggioranza, che non è stata raggiunta (se ne sarebbero dovuti compromettere 4 su 7). Alla prova dei fatti il servizio di directory di Tor si è quindi confermato robusto.]
4. [l'unica possibilità reale di alterazione del funzionamento di Tor, anche se non confermata ma possibile, è che siano state fornite informazioni alterate sui nodi relay, e che perciò alcuni utenti dei nodi relay possano essere stati compromessi.]

Se fosse realmente successo, potrebbe aver aiutato qualche cinese sfortunato che avesse selezionato ed usato un relay in quei pochi giorni, a finire dietro le sbarre, visto che i relay nodes sono nati come reazione alla censura cinese sui contenuti della Rete.

Si deve notare però che:- non c'è evidenza positiva che questo sia accaduto: è solo una possibilità, che è durata solo per pochi giorni- i nodi relay funzionanti all'inizio di gennaio erano comunque in numero limitato- l'intervallo di vulnerabilità è stato ridotto a pochi giorni dall'aggiornamento di Tor distribuito prima che la notizia fosse resa pubblica.

Si può concludere che il gruppo dei core developer del progetto Tor ha reagito all'intrusione in maniera estremamente efficace, professionale e soprattutto con completa disclosure, e questa, a mio parere è un'ottima notizia.

Ognuno poi sarà libero di formarsi la propria opinione: va considerato che fatti anche molto più gravi di questo sono già successi e succedono ancora oggi.

Ricordate il caso dell'attacco mirato e malizioso portato anni or sono (nel 2003) ai sorgenti del kernel di Linux? Un singolo carattere aggiunto ad una singola riga del kernel avrebbe permesso, se non rilevato, di compromettere qualsiasi macchina Linux; questo attacco è stato seguito da altri almeno fino al 2008. Li trovate riassunti in questo e quest'altro articolo, ambedue apparsi su *Cnet*.

Non per voler guardare solo la bottiglia mezza piena, ma personalmente ritengo che un evento di questo tipo, rilevato e superato senza grossi danni, confermi la validità del modello di sviluppo open del software, e della full disclosure dei problemi e degli attacchi rilevati.

Cosa succeda invece nel mondo del software closed può solo essere oggetto di cupe congetture, ma se tanto mi dà tanto…

P.S. se ce ne fosse bisogno, sottolineo la necessità di aggiornare subito i vostri nodi Tor, per ripristinare l'accesso a tutti e 7 i dirserver, incluso i 2 nuovi che hanno sostituito quelli compromessi.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on August 30, 2023.

Canonical link

Exported from Medium on January 2, 2024.